

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A security document, comprising:
a printed document; and
one or more memory circuits configured to be read wirelessly and attached to or incorporated within the printed document at a predetermined position or positions with respect to the printed document,
wherein data in each of the one or more memory ~~circuit~~ circuits is protected from access by an unauthorized reader,
wherein each of the one or more memory ~~circuit~~ circuits is physically isolated so as to inhibit physical tampering or is configured to indicate when physical tampering has occurred, and
wherein physical isolation of each of the one or more memory ~~circuit~~ circuits employs one or more tamper-evident strips, and
wherein each of the one or more memory circuits provides security for a portion of the printed document adjacent to the respective one or more memory circuits.
2. (Currently Amended) A security document as claimed in claim 1, wherein each of the one or more memory ~~circuit~~ circuits is inductively powered.
3. (Currently Amended) A security document as claimed in claim 2, wherein each of the one or more memory ~~circuit~~ circuits receives and transmits data wirelessly at radio frequency.
4. (Cancelled)
5. (Currently Amended) A security document as claimed in claim 1, wherein each of the one or more memory ~~circuit~~ circuits includes an antenna that is configured for detection or resistance of physical tampering.

6. (Previously Presented) A security document as claimed in claim 1, wherein the security document is configured to identify an authorized bearer of the security document.

7. (Previously Presented) A security document as claimed in claim 6, wherein the security document includes means to allow access to a specified asset or assets by the authorized bearer.

8. (Currently Amended) A method of publishing a security document, comprising:

- a. determining first information for printing in a printed document, and second information for writing to one or more memory circuits for attachment to or incorporation within the printed document at a predetermined position or positions with respect to the printed document;
- b. protecting the second information from unauthorized reading;
- c. printing the first information in the printed document;
- d. writing the second information to one or more memory circuits configured to be read wirelessly for attachment to or incorporation within the printed document; and
- e. physically isolating the one or more memory circuits so as to inhibit physical tampering or configuring the one or more memory circuits to indicate when physical tampering has occurred,

wherein each of the one or more memory circuits provides security for a portion of the printed document adjacent to the respective memory circuit.

9. (Currently Amended) A method of reading a security document comprising a printed document and one or more memory circuits attached to or incorporated within the printed document, comprising:

- a. obtaining authorization information to read the security document;
- b. reading first information printed in the printed document;

- c. wirelessly powering at least one memory circuit and wirelessly reading protected second information stored in said memory circuit;
- d. reading, by a document reader device, the second information by using the authorization information; and
- e. using the second information with the first information to assess the security document.

10. (Original) A method as claimed in claim 9, further comprising comparing the second information to one or more characteristics of a bearer of the security document.

11. (Currently Amended) A security document, comprising:
a printed document; and

one or more memory circuits configured to be read wirelessly attached to or incorporated within the printed document at a predetermined position or positions with respect to the printed document,

wherein data in each of the one or more memory ~~circuit~~ circuits is protected from access by an unauthorized reader,

wherein each of the one or more memory ~~circuit~~ circuits is physically isolated so as to inhibit physical tampering or is configured to indicate when physical tampering has occurred, and

wherein both printed data and data in each of the one or more memory ~~circuit~~ circuits is configured to identify a bearer of the security document,

wherein each of the one or more memory circuits provides security for a portion of the printed document adjacent to the respective memory circuit.

12. (Currently Amended) A method of publishing a security document for a bearer, comprising:

- a. determining first information concerning the bearer for printing in a printed document, and second information concerning the bearer for writing to one or more memory circuits for attachment to or incorporation within the printed document;
- b. protecting the second information from unauthorized reading;

- c. printing the first information in the printed document;
- d. writing the second information to one or more memory circuits configured to be read wirelessly for attachment to or incorporation within the printed document at a predetermined position or positions with respect to the printed document; and
- e. physically isolating each of the one or more memory circuits in the printed document so as to inhibit physical tampering or to indicate when physical tampering has occurred,

wherein each of the one or more memory circuits provides security for a portion of the printed document adjacent to the respective memory circuit.

13. (Currently Amended) A security document as claimed in claim 1, wherein the one or more tamper-evident strips provide a visual indication as to whether or not the one or more memory ~~circuit~~ circuits has been physically tampered with.

14. (Currently Amended) A security document as claimed in claim 1, wherein the one or more tamper-evident strips correspond to at least one cut on the printed document provided adjacent to the one or more memory ~~circuit~~ circuits.

15. (Previously Presented) A security document as claimed in claim 1, wherein the printed document is a sheet of paper.

16. (Previously Presented) A security document as claimed in claim 11, wherein the printed document is a sheet of paper.

17. (Previously Presented) A method as claimed in claim 12, wherein the printed document is a sheet of paper.

18. (Previously Presented) A security document as claimed in claim 1, wherein the one or more memory circuits are provided on an external surface of the printed document that is exposed to the environment.

19. (Previously Presented) A security document as claimed in claim 11, wherein the one or more memory circuits are provided on an external surface of the printed document that is exposed to the environment.

20. (Previously Presented) A method as claimed in claim 12, further comprising:

providing the one or more memory circuits on an external surface of the printed document that is exposed to the environment.

21. (Currently Amended) A security document ~~as claimed in claim 5~~, comprising:
a printed document; and
one or more memory circuits configured to be read wirelessly and attached to or
incorporated within the printed document,
wherein data in the memory circuit is protected from access by an unauthorized
reader,
wherein the memory circuit is physically isolated so as to inhibit physical tampering
or is configured to indicate when physical tampering has occurred,
wherein physical isolation of the memory circuit employs one or more tamper-evident
strips
wherein the memory circuit includes an antenna that is configured for detection or
resistance of physical tampering, and
wherein the memory circuit includes means for detecting a change in a physical property of the antenna, the change in the physical property being indicative of physical tampering of the antenna, wherein the memory circuit includes means for disabling reading of the memory circuit when the physical tampering of the antenna is detected.

22. (Previously Presented) A security document as claimed in claim 1, wherein the memory circuit includes tamper resistance means for resisting tampering of the memory circuit.

23. (Currently Amended) A method ~~according to claim 8,~~ of publishing a security document, comprising:

a. determining first information for printing in a printed document, and second information for writing to one or more memory circuits for attachment to or incorporation within the printed document;

b. protecting the second information from unauthorized reading;

c. printing the first information in the printed document;

d. writing the second information to one or more memory circuits configured to be read wirelessly for attachment to or incorporation within the printed document;

e. physically isolating the one or more memory circuits so as to inhibit physical tampering or configuring the one or more memory circuits to indicate when physical tampering has occurred, wherein the one or more memory circuits including an antenna that is configured for detection or resistance of physical tampering [[,]];

~~the method further comprising:~~

f. detecting a change in a physical property of the antenna, the change in the physical property being indicative of physical tampering of the antenna; and

g. disabling reading of the memory circuit when the physical tampering of the antenna is detected.

24. (Currently Amended) A security document ~~according to claim 11,~~ comprising: a printed document; and

one or more memory circuits configured to be read wirelessly attached to or incorporated within the printed document,

wherein data in the memory circuit is protected from access by an unauthorized reader,

wherein the memory circuit is physically isolated so as to inhibit physical tampering or is configured to indicate when physical tampering has occurred,

wherein both printed data and data in the memory circuit is configured to identify a bearer of the security document,

wherein the memory circuit includes an antenna that is configured for detection or resistance of physical tampering, and

wherein the memory circuit includes means for detecting a change in a physical property of the antenna, the change in the physical property being indicative of physical tampering of the antenna, wherein the memory circuit includes means for disabling reading of the memory circuit when the physical tampering of the antenna is detected.

25. (Currently Amended) A method ~~according to claim 12, of publishing a security document for a bearer, comprising:~~

a. determining first information concerning the bearer for printing in a printed document, and second information concerning the bearer for writing to one or more memory circuits for attachment to or incorporation within the printed document;

b. protecting the second information from unauthorized reading;

c. printing the first information in the printed document;

d. writing the second information to one or more memory circuits configured to be read wirelessly for attachment to or incorporation within the printed document;

e. physically isolating the one or more memory circuits in the printed document so as to inhibit physical tampering or to indicate when physical tampering has occurred, wherein the one or more memory circuits including an antenna that is configured for detection or resistance of physical tampering,

the method further comprising:

f. detecting a change in a physical property of the antenna, the change in the physical property being indicative of physical tampering of the antenna; and

g. disabling reading of the memory circuit when the physical tampering of the antenna is detected.

26. (New) A security document as claimed in claim 1, wherein the one or more memory circuits comprises at least two memory circuits.

27. (New) A method as claimed in claim 8, wherein the one or more memory circuits comprises at least two memory circuits.

28. (New) A security document as claimed in claim 12, wherein the one or more memory circuits comprises at least two memory circuits.

29. (New) A method as claimed in claim 12, wherein the one or more memory circuits comprises at least two memory circuits.